Cybersecurity & Infrastructure Health Check

Fortify Your Defenses in One Week

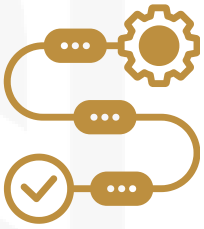
$5,000 Fixed Fee

In today's rapidly evolving threat landscape, safeguarding your organization's critical assets demands a proactive approach. Our comprehensive one-week Cybersecurity and Infrastructure Health Check empowers you with actionable insights to strengthen your security posture and ensure operational resilience.

What We Evaluate:

- **Security Evaluation:**
  - **Governance and Risk Management:** Review policies and risk assessments to identify potential weaknesses
  - **Resiliency Planning:** Assess business continuity and incident response plans for preparedness and effectiveness
  - **Vulnerability and Penetration Assessments:** Review existing assessments and reports to identify and prioritize vulnerabilities
  - **Data Privacy & Sensitive Data Management:** Evaluate your organization's data protection measures, including encryption, access controls, and data handling policies. Assess compliance with state privacy regulations such as CCPA, CPA, and VCDPA to ensure robust protection of sensitive data
  - **Third-Party Vendor Management:** Evaluate the security practices and potential risks associated with your third-party vendors, including their data handling, access controls, and incident response capabilities
  - **Security Monitoring:** Evaluate the effectiveness of your security monitoring tools (e.g., SIEM, SOC)
  - **Physical Security:** Review physical access controls and environmental safeguards to protect critical assets
- **Infrastructure Evaluation:**
  - **IT Help Desk/MSP:** Assess the efficiency of your IT help desk or your MSP, including response times, knowledge base resources, and user satisfaction
  - **Email Security, Anti-Virus, and MFA:** Review your Microsoft 365 or Google Suite email security measures, anti-malware solutions, and multi-factor authentication implementation to evaluate their effectiveness in protecting against cyber threats
  - **Patch Management:** Assess patch deployment processes and identify potential vulnerabilities
  - **Asset Management:** Review your IT asset management practices for comprehensive visibility and control over your IT environment
  - **Identity and Access Management (IAM):** Evaluate access controls, authentication mechanisms, and user provisioning
  - **Backup and Disaster Recovery:** Assess the effectiveness of backup procedures, recovery capabilities, and data restoration
  - **Enterprise Applications:** Inventory applications, including ERP, CRM, and HRIS, to identify security risks
  - **Cloud and On-Premise Data Centers:** Evaluate security controls and data protection measures in both environments

- **Our Process:**
  - **Comprehensive Evaluation:** Conduct a thorough review of your cybersecurity and infrastructure controls. This process typically takes 3-4 days
  - **Gap Identification:** Identify areas for improvement and potential vulnerabilities across your IT and security landscape. This process typically takes 1-2 days
  - **Roadmap Development:** Provide a detailed, actionable roadmap prioritizing remediation efforts and aligning your systems with best practices. This process typically takes 1-2 days



- **Benefits:**
  - **Risk Mitigation:** Minimize downtime and protect your organization from potential threats
  - **Actionable Insights:** Receive clear guidance on how to enhance your cybersecurity posture
  - **Compliance Assurance:** Ensure your organization meets regulatory requirements and industry standards
  - **Cost-Effective & Efficient:** Receive a comprehensive assessment at a fixed fee of $5,000 with a fast turnaround time of one week
  - **Peace of Mind:** Gain confidence in your infrastructure and cybersecurity defenses

How Can We Help?

To schedule your complimentary 30-minute session with our team, please click this link to **schedule your meeting**.

dla@dlallc.com | 973-575-1565 | www.dlallc.com

Fairfield, NJ | New York, NY | Shrewsbury, NJ | Boston, MA | Chicago, IL